Department of Homeland Security Daily Open Source Infrastructure Report for 10 July 2007

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- IDG News reports that according to Symantec, credit card thieves are starting to use charitable donations with stolen credit cards as a final check to ensure that the numbers will work. (See item 9)
- GovExec reports the Secure Border Initiative Network −− a wireless network of high−tech towers to watch for illegal immigrants crossing from Mexico −− is vulnerable to cyber attacks that could shut the system down. (See item 13)
- New York police officials say that by the end of this year more than 100 cameras will be monitoring cars moving through Lower Manhattan, in the beginning phase of the Lower Manhattan Security Initiative, a London−style surveillance system that would be the first in the United States. (See item 33)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *July 09, Wall Street Journal* — **IEA warns of impending crunch in gas supply.** In a dire forecast, the International Energy Agency (IEA) is warning of an impending crunch in the supply of oil and natural gas needed to power world economic growth in coming years. The

IEA is the energy watchdog of the world's 26 most−advanced economies, and its pessimistic assessment is contained in its latest annual medium−term forecast to 2012. The agency expects oil supply to be tighter in coming years than it had previously forecast, with little prospect of relief except a possible easing should world economic growth falter. The IEA now forecasts that the Organization of Petroleum Exporting Countries will have precious little spare capacity left to pump extra oil by 2012. It also expects supply increases from non−OPEC oil producers and biofuel producers to start flagging after 2009. Natural−gas markets will also be tight because of inadequate supply increases, limiting the ability of consumers to switch between oil and natural gas. Still, demand for oil and gas is expected to grow at a brisk pace in the years to 2012.
Source: http://online.wsj.com/article/SB118397769578260737.html?mod= googlenews_wsj

2. *July 09, Associated Press* — **U.S. oil companies' influence wanes.** Developing countries are locking up a bigger share of the world's oil and gas resources to profit from high prices and fuel industrial growth. Some experts view the shift as an emerging threat to the U.S. economy, while others see benefits for consumers, saying an expanding list of suppliers diminishes the impact of any single disruption. New research by investment bank Goldman Sachs suggests four countries in particular −− Brazil, Russia, India and China, or the so−called BRIC countries −− are grabbing the most market share from American companies. The BRIC's share of the industry's market value has grown from virtually nothing 15 years ago to more than one third today, while American companies' stake has dwindled from more than half to less than a third. The biggest factor, most analysts agree, is the growth of state−controlled national oil companies, including PetroChina Ltd., an arm of China National Petroleum Corp.; Russia's OAO Gazprom, the world's biggest natural gas producer; and Brazil's Petroleo Brasileiro SA, or Petrobras. Whether this trend is bad for America's long−term strategic interests is debated by analysts and executives.
Source: http://biz.yahoo.com/ap/070706/american_energy.html?.v=1

3. *July 08, Agence France−Presse* — **Libya to open up gas fields to foreigners.** Libya on Sunday, July 8, invited international tenders for exploration of its onshore and offshore gas fields covering an area almost the size of Scotland. The National Oil Company is offering a dozen contracts to explore 41 gas blocks in the Mediterranean, the Sirte basin in the north−central area of the country, Cyrenaica further east and Murzek and Ghdamess in the south. The blocks cover almost 28,000 square miles, it said in a statement. OPEC member Libya is the African continent's second largest oil producer at 1.7 million barrels per day. It also has natural gas reserves estimated at 46,403 billion cubic feet. With the end of sanctions after Libyan leader Moamer Kadhafi's decision in December 2003 to abandon weapons of mass destruction programs, oil and gas exploration in the north African country has picked up at a frenetic pace.
Source: http://news.yahoo.com/s/afp/20070708/bs_afp/libyaenergygas_070708214743;_ylt=Auab09wTtEEF3UJQbRnoU4KmOrgF

4. *July 06, Associated Press* — **Worker safety concerns at BP facility.** Alaska state labor department officials said they are reviewing congressional concerns about alleged safety risks at a natural gas processing facility operated by BP PLC in Prudhoe Bay. Among the allegations is that the facility is holding nearly double its safe capacity, putting workers' lives at risk. State officials have said the London−based company plans to back up claims they made to Alaska

Occupational Safety and Health officials that there is no imminent danger to the plant's work force or any other area workers. More than 200,000 gallons of oil leaked at Alaska's Prudhoe Bay field in March 2006 due to corrosion. Five months later, after another leak, BP partially shut down the nation's largest oil field, which it operates on behalf of itself, ConocoPhillips and Exxon Mobil Corp. BP has pledged to replace 16 miles of corroded pipeline by the end of next year at a cost of about $250 million.
Source: http://biz.yahoo.com/ap/070706/wst_bp_alaska.html?.v=1

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *July 09, Associated Press* — **Navy reasserting control of shipbuilding.** Stung by cost overruns, the Navy is looking to return to a past when it controlled the shipbuilding process from beginning to end. The change follows a period when the Navy told shipyards what it wanted the ships to do and then let them deliver rather than getting mired in design details. But that approach failed to control costs in construction of the speedy Littoral Combat Ship for close−to−shore operations and in the design of the stealthy DDG−1000 destroyer. Starting in the spring, Navy Secretary Donald Winter has been making the case for what he describes as "tough love" for the shipbuilding industry. "The Navy must reassert its control over the entire shipbuilding acquisition process. The Navy owns the fleet, and the Navy is the customer. Sometimes one has the impression that this tiny distinction has been forgotten," Winter wrote in an essay last month. However, some say cost overruns are inevitable as the Navy launches new classes of warships. Unlike other defense contractors, shipbuilders don't have the luxury of building prototypes. The first warship of a new class is the prototype of sorts and thus prone to unexpected problems during design and construction.
Source: http://biz.yahoo.com/ap/070709/shipbuilding_woes.html?.v=2

[Return to top]

Banking and Finance Sector

6. *July 09, Bloomberg* — **Banks' costs to prevent laundering exceed forecasts.** Banks' costs to prevent money laundering have "increased substantially" in the last three years, driven by regulation and increasing risks in emerging markets, a survey by KPMG International found. Average prevention costs jumped 58 percent in the last three years, exceeding predictions of a 43 percent gain, the survey of 224 banks and senior executives found. North American banks had the biggest increases, with costs up an average of 71 percent. Britain and other countries tightened money−laundering rules after the September 11, 2001, attacks to prevent financial terrorism. Increased scrutiny has forced banks to boost spending to enforce money laundering rules in recent years. Estimated money laundering flows may be more than one trillion dollars

annually, KPMG said, citing a U.S. report to Congress.
Source: http://www.bloomberg.com/apps/news?pid=20601102&sid=a3Vh_wOTrKc8&refer=uk

7. *July 09, Computer World UK* — **New tool lets criminals set up phishing sites in seconds.** A new 'plug and play' phishing kit can let fraudsters create phishing site in two seconds, has been found by security firm RSA. The security firm's Anti−Fraud Command Center (AFCC) has discovered what it calls a "plug−and−play" phishing kit, which can create a fully functional phishing site on a compromised server in two seconds, once double−clicked on. The kit consists of a single electronic file that fraudsters can upload to a server. The traditional method of creating phishing sites involves installing various files one−by−one in corresponding directories. This process requires multiple visits to the compromised server and manual installation, which increases the chance of detection, says RSA. This new development in online fraud could also enable online attackers to automatically search for vulnerable servers without actually hacking into the server, warned RSA Security in its Monthly Online Fraud Report. The RSA AFCC detects, monitors and shuts down phishing, pharming and Trojan attacks for around 200 institutions worldwide.
Source: http://www.computerworlduk.com/management/security/cybercrime/news/index.cfm?newsid=3902

8. *July 08, Associated Press* — **Police seek leads in state computer theft.** Police investigating the theft of a computer backup device containing personal information on Ohio state employees and family members are going door−to−door and mailing postcards with tip line information to dig up new leads. The device was stolen June 10 from a state intern's unlocked car at an apartment complex. The tape contained personal information on state employees and the names and Social Security numbers of 225,000 taxpayers. As of Friday, July 6, about 59,000 people had started the process of enrolling in identity−theft protection services offered through the state, said Ron Sylvester, spokesperson for the Ohio Department of Administration Services.
Source: http://www.chroniclet.com/2007/07/08/police−seek−leads−in−st ate−computer−theft/

9. *July 06, IDG News Service* — **Scammers use charities to test credit cards.** Credit card thieves are becoming big−time charity donors, but it's not out of the goodness of their hearts. According to Symantec, the criminals are starting to use charitable donations as a way to check whether their stolen credit card numbers are working. Fraudsters have been using a similar technique for years, but until recently, they tended to make minor purchases on online retail sites. Now, as these sites have become better at identifying and blocking these transactions, the criminals have begun looking elsewhere, said Zulfikar Ramzan, senior principal researcher with Symantec. "Using a charitable organization as a way to verify a credit card number is a relatively new technique, and it's probably being used by a minority of the more innovative guys," he said. Credit card numbers are bought and sold in underground "carder" forums, which bring together the people who have stolen the credit card numbers with those who want to use them. These charitable donations are typically made by the person buying the card numbers as a final check to ensure that the numbers will work, Ramzan said.
Source: http://www.infoworld.com/article/07/07/06/Fraudsters−use−charities−to−test−credit−cards_1.html

[Return to top]

Transportation and Border Security Sector

10. *July 10, Stuff.co.nz (New Zealand)* — **Pat−downs, testing planned for passengers.** Passengers leaving New Zealand as well as airport workers will face tighter screening under new aviation laws to be enacted from August 1. As part of the crackdown, airport workers will be screened and searched in the same manner as passengers. At present, no formal procedures are in place for screening and searching people who work at airports. Although passengers and crew boarding aircraft are screened, those who have access to baggage and in−service aircraft are not. Ministry of Transport spokesperson Peter Burke said airport workers who entered "sterile areas" (the area between the screening point and the departure gate) must go through the same screening as passengers entering that area. "Random screening of airport workers in other areas of the airport will be introduced later this year when the Aviation Security Legislation Bill has been passed," he said. Aviation Security Services general manager Mark Everitt said all passengers would be randomly tested for explosives using "trace detection" technology. Luggage is already screened for traces of explosives, but the new testing equipment will be able to detect a wider range of explosives.
Source: http://www.stuff.co.nz/4122143a11.html

11. *July 09, Department of Transportation* — **Department of Transportation seeks comments on airline bumping rule.** The Department of Transportation on Monday, July 9, asked for public comment on possible changes to the rules governing airline oversales, or “bumping,” including a possible increase in the maximum compensation due to passengers bumped from oversold flights. The bumping rules were first adopted in 1962 to balance the rights of passengers with the needs of air carriers to minimize the effect of passengers with reservations who do not take their flight. If a flight is oversold, the airline must first seek volunteers who are willing to give up their seats in return for compensation offered by the airline. The airline may bump passengers involuntarily if not enough of them volunteer, and these passengers are eligible for cash compensation in most circumstances. The rule applies to passengers bumped from an oversold flight that departs without them, not to those affected by delayed or canceled flights. The Department’s notice also asked for comment on other possible changes to the bumping rule, such as extending the rule to aircraft having 30 to 60 seats, which are not currently covered, and clarifying the criteria airlines may use in deciding the order in which passengers will be bumped.
Further information on bumping rules:
http://airconsumer.ost.dot.gov/publications/flyrights.htm#ov erbooking
Source: http://www.dot.gov/affairs/dot6707.htm

12. *July 06, Associated Press* — **Man arrested at airport carrying knife, stun gun and Mace.** An Illinois man dressed in disguise was arrested at Minneapolis−St. Paul International Airport and charged with plotting to kidnap his former girlfriend when she got off a flight, according to a criminal complaint. Timothy J. Pentaleri, 42, of Belleville, IL, was arrested June 29 after police became suspicious and approached him. He was wearing a heavy brown coat and, it turned out, a wig and a fake mustache and beard. When officers frisked him, they found a stun gun, Mace, a knife, and a baton, according to the complaint filed Thursday, July 5, in Hennepin County District Court. Later, police searched Pentaleri's vehicle at the airport and found a shovel, handcuffs, duct tape, and other items, including a handwritten note saying he would

stun the woman and "club her hard," according to the complaint. They also found a duffel bag containing condoms, a pillowcase cut into strips and other items.
Source: http://www.kare11.com/news/ts_article.aspx?storyid=259259

13. *July 06, GovExec* — **High−tech border network could fall prey to cyber attacks.** The Department of Homeland Security's (DHS) planned wireless network of high−tech towers to watch for illegal immigrants crossing the border from Mexico into the United States is vulnerable to cyber attacks that could shut the system down, according to security experts. The Secure Border Initiative Network (SBInet) surveillance system, a network of 1,800 towers housing infrared cameras, radar and communication equipment along the U.S.−Mexican border that DHS just began testing, will use commercial wi−fi systems to connect the towers to command−and−control centers operated by U.S. Customs and Border Protection and to computers in vehicles operated by border agents. But shortly after the SBInet towers went up 28 miles of the border southwest of Tucson, in mid−June, they started knocking out wireless Internet service in Arivaca, AZ, a town of about 1,500 residents located 12 miles north of the Mexican border. Allan Wallen, who runs a wireless Internet service provider cooperative serving Arivaca, said the contractor was using the 5.8 gigahertz wi−fi band (also known as industry standard 802.11a) for communications on the SBInet towers −− the same frequency the ISP used to provide Internet service. Using standard commercial 5.8 gigahertz wi−fi equipment could leave SBInet open to intentional interference.
Source: http://www.govexec.com/story_page.cfm?articleid=37393&dcn=to daysnews

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

14. *July 08, Associated Press* — **Disease outbreak alarms Montana's ranchers.** The future of Montana's cattle industry, some say, is in the hands of the federal government and a Bridger ranching couple. Ranchers and livestock groups from the state and around the country are anxiously watching negotiations between Jim and Sandy Morgan and the U.S. Department of Agriculture's Animal and Plant Health Inspection Service over the couple's quarantined cattle. Seven cows from their ranch tested positive for brucellosis in May, and Montana could lose its coveted brucellosis−free status if the Morgans' herd isn't slaughtered within 60 days of that discovery −− which is July 17. Concerns are mounting that a deal won't be reached in time. Hayley Carraway, communications manager for the Montana Stockgrowers Association, said the state's brucellosis−free status is critical to its livestock industry. Losing it would cost producers business in other states and subject them to expensive testing and vaccination programs, possibly for years. Brucellosis, which causes pregnant cows to abort their calves, was widely eradicated from livestock last century but has persisted in wildlife such as elk and bison. Recent outbreaks in Idaho and Wyoming have cost livestock producers there millions of dollars. What's holding up the Bridger cattle herd deal is a price for the animals.

Source: http://seattletimes.nwsource.com/html/localnews/2003779622_b rucellosis08.html

15. *July 07, Associated Press* — **Minnesota bull dies of anthrax.** A bull in Marshall, MN, has died from anthrax −− marking the first case of the disease in 2007, authorities confirmed. The state Board of Animal Health said on Thursday, July 5, that the bull was found dead in a pasture last week. Tests confirmed that the bull had anthrax. The herd had not been vaccinated for anthrax this year. The herd has since been taken out of the pasture where the infection occurred and has been placed under quarantine for 30 days from the day the bull died. Last year was the second−worst year for anthrax deaths in Minnesota. A total of 91 animals died on 28 farms in northwestern Minnesota.
Source: http://www.postbulletin.com/newsmanager/templates/localnews_story.asp?a=300033&z=2

16. *July 06, U.S. Department of Agriculture* — **Additional funding for emerald ash borer and potato cyst nematode eradication.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Friday, July 6, announced the availability of an additional $11.3 million in emergency funding for the emerald ash borer (EAB) program and $500,000 for the potato cyst nematode (PCN) program in Idaho. USDA will provide this emergency funding to states with established EAB programs and quarantines to support pest detection, control, regulation of host material that will mitigate the risk of further spread of the pest, as well as outreach and education to the general public. A portion of the funding will also be provided to targeted uninfested states at risk for EAB for additional survey and response if a detection of the pest should occur. EAB is an invasive species of wood−boring beetles that has been responsible for the death and decline of more than 25 million ash trees in the U.S. The $500,000 for PCN is in addition to nearly $24 million in emergency funding that has already been dedicated toward PCN surveillance and eradication activities in Idaho. The funding will advance intensive survey activities in seed potato fields, packing facilities and storage sheds. PCN primarily affects plants within the potato family including tomatoes and eggplants. PCN can cause up to 80 percent yield loss.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2007/07/0193.xml

[Return to top]

Food Sector

17. *July 09, Reuters* — **China says food safety scares threaten stability.** China risks damaging its global credibility and provoking social instability if it does not tackle its food and drug quality problems, an official said in a rare admission amid a series of scares over tainted products. China's safety failings have drawn world attention since mislabeled chemical exports were found in cough syrup in Panama and pet food in the U.S. In one of the most recent, the U.S. Food and Drug Administration said it would not allow imports of Chinese farm−raised seafood unless suppliers could prove the shipments held no harmful residues. "The food security problems have impeded Chinese agri−products and food many times in international trade, and damaged our national credibility and image," Sun Xianze, director of food safety coordination at the State Food and Drug Administration, said. "The occurrence of food safety incidents or cases not only affects the healthy development of the whole industry, but also may impact upon economic and social stability," Sun was quoted as saying by state media.

Source: http://www.sciam.com/article.cfm?alias=china−says−food−safety−sc&chanId=sa003&modsrc=reuters

[Return to top]

Water Sector

18. *July 08, Xinhua (China)* — **Digging water tunnels starts beneath Yellow River.** A ground−breaking ceremony was held on Sunday, July 8, as construction began on a pair of tunnels −− part of the massive south−to−north water diversion project −− that will traverse the Yellow River and bring Yangtze River water all the way to Beijing. The two tunnels will be 4,250 meters long and have a diameter of seven meters. They will pass underneath the Yellow River to the west of Zhengzhou, the provincial capital of Henan Province, according to builders. The project will divert water from the Yangtze River, China's longest river, to the thirsty north of the country. Three routes are planned −− eastern, middle and western.
Source: http://news.xinhuanet.com/english/2007−07/08/content_6345328 .htm

19. *July 08, Associated Press* — **Contaminated water, oil raise health concerns for Coffeyville.** As Coffeyville, KS, residents continued to regroup Saturday, July 7, a week after floodwaters inundated their homes and businesses, the government raised new concerns about health problems from the contaminated water and its residue. Lawns, houses and ballfields on the city's east side were streaked with blackish oily stains left behind after 71,400 gallons of crude oil spilled from the Coffeyville Resources refinery because of a malfunction while the refinery shut down before the flooding along the Verdigris River. The U.S. Environmental Protection Agency announced that two floodwater samples from Coffeyville showed the level of fecal coliform bacteria was more than 130 times the standard. The bacteria can cause stomachache, fever, vomiting and diarrhea, the agency said. "We have several concerns for the residents of Coffeyville," said Sue Casteel, environmental scientist for the Agency for Toxic Substances and Disease Registry. "What we observed with people who came in contact with oil at Katrina was they would develop rashes and red flaky skin."
Source: http://www2.ljworld.com/news/2007/jul/08/contaminated_water_oil_raise_health_concerns_coffe/

[Return to top]

Public Health Sector

20. *July 09, Associated Press* — **Indonesian boy dies of bird flu.** An Indonesian boy died of bird flu, bringing the death toll to 81 in the only country regularly logging human fatalities from the virus, a health official said Monday, July 9. The six−year−old boy died Sunday, July 8, at a hospital in the capital of Jakarta, said Rumizar Rusin of the Health Ministry's bird flu information center. The boy fell sick on July 1 and was admitted to the hospital four days later, he said. Rusin said officials were still investigating how the boy contracted the H5N1 virus.
Source: http://www.iht.com/articles/ap/2007/07/09/asia/AS−GEN−Indone sia−Bird−Flu.php

21.

July 08, Agence France−Presse — **Dengue fever cases up 36 percent in Thailand.** Cases of dengue fever in Thailand have risen 36 percent since last year, local press reported Sunday, July 8, as an epidemic of the mosquito−borne disease swept the region. The outbreak has killed 17 people in Thailand and affected more than 21,000 since the beginning of the year, the Nation newspaper reported, quoting figures from the health ministry. Dengue fever is on the rise across Southeast Asia. In Cambodia, which borders Thailand, at least 132 people have died this year, while wealthy Singapore has seen 3,597 cases and three deaths.
Source: http://news.yahoo.com/s/afp/20070708/hl_afp/thailandhealthillness_070708210456;_ylt=Aj2TQjPXwww_H476uskBAGGJOrgF

22. *July 06, Massachusetts Institute of Technology* — **Team builds viruses to combat harmful biofilms.** In one of the first potential applications of synthetic biology, an emerging field that aims to design and build useful biomolecular systems, researchers from the Massachusetts Institute of Technology (MIT) and Boston University are engineering viruses to attack and destroy the surface "biofilms" that harbor harmful bacteria in the body and on industrial and medical devices. They have already successfully demonstrated one such virus, and thanks to a "plug and play" library of "parts" believe that many more could be custom−designed to target different species or strains of bacteria. The work helps vault synthetic biology from an abstract science to one that has proven practical applications. Bacterial biofilms can form almost anywhere. When they accumulate in hard to reach places such as the insides of food processing machines or medical catheters, however, they become persistent sources of infection. These bacteria excrete a variety of proteins, polysaccharides, and nucleic acids that together with other accumulating materials form an extracellular matrix that encases the bacteria.
Source: http://web.mit.edu/newsoffice/2007/biofilm−0706.html

23. *July 03, GovernmentHealthIT* — **Health agencies debut Website for NHIN tools, resources.** The agencies involved in setting up the National Health Information Network (NHIN) has debuted a Website designed to provide tools, information and resources for companies and public organizations seeking to conform their systems to emerging NHIN standards. The Website was developed by the Certification Commission for Healthcare Information Technology (CCHIT), the Healthcare IT Standards Panel (HITSP), the National Institute of Standards and Technology, and the Office of the National Coordinator for Health IT. The site contains information about NHIN initiatives, including standards, specifications and testing resources.
Source: http://govhealthit.com/article103139−07−03−07−Web

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

24.

July 05, St. Louis Post−Dispatch — **All companies need a disaster recovery plan.** A prolonged power outage like St. Louis experienced multiple times last year is a major inconvenience for homeowners, but it can be lethal to businesses. The National Archives and Records Administration says 93 percent of companies that lose access to their data for 10 days or more file for bankruptcy within one year. But companies can develop an emergency preparedness plan that works for them. A key component in any business's emergency preparedness plan is protecting the information stored in its computers. Information technology is at the core of critical business processes, making a contingency plan essential, said Elizabeth Niedringhaus, president of SSE Inc., a St. Louis company that develops courseware and data software, designs networks for companies and offers technology services to businesses. Niedringhaus stressed the need to develop a contingency plan listing measures a business must take to recover information technology services after an emergency or system disruption. That includes backup methods and options, alternate sites, equipment replacement and places to keep copies of software, she said.
Source: http://www.stltoday.com/stltoday/business/stories.nsf/0/A638B34271B441908625730E00048181?OpenDocument

[Return to top]

Information Technology and Telecommunications Sector

25. *July 09, IDG News Service* — **Average zero−day bug has 348−day lifespan, exec says.** The average zero−day bug has a lifespan of 348 days before it is discovered or patched, but some vulnerabilities live on for much longer, according to security vendor Immunity's chief executive officer. Zero−day bugs are vulnerabilities that have not been patched or made public. When discovered and not disclosed, these bugs can be used by hackers and criminals to break into corporate systems to steal or change data. As a result, there is a thriving market for zero−day bugs. "Huge amounts of money are being offering to zero−day discoverers for their zero−days," said Justine Aitel, Immunity's CEO, speaking in Singapore at the SyScan '07 security conference. Immunity, which buys but does not disclose zero−day bugs, keeps tabs on how long the bugs it buys last before they are made public or patched. While the average bug has a lifespan of 348 days, the shortest−lived bugs are made public in 99 days. Those with the longest lifespan remain undetected for 1,080 days. To protect their data, security executives need to dig out the zero−day bugs in their systems, Aitel said, noting that this is an area most companies ignore.
Source: http://www.infoworld.com/article/07/07/09/zero−day−bug−lifes pan_1.html

26. *July 09, IDG News Service* — **Google to buy Postini for $625 million.** Google has agreed to buy messaging security company Postini for $625 million in a move to increase the appeal of Google's hosted applications among big businesses, the companies announced on Monday, July 9. Postini provides messaging security, archiving, policy enforcement and other services to about 35,000 business customers around the world, Google said. The vendor plans to use the technology to boost the security and compliance features of Google Apps, its hosted suite of productivity applications.
Source: http://news.yahoo.com/s/infoworld/20070709/tc_infoworld/90049;_ylt=AhsVUtQUgfrzLRFcyt4PIN0jtBAF

27. *July 09, Websense Security Labs* — **Malicious Websites / Malicious Code: New fake patch malicious code run.** Websense Security Labs has received reports that a new e−mail campaign is spreading that attempts to lure users into downloading malicious code. It appears as though the same group that was behind the widespread attacks July 4th, that used greeting card lures to spread, are behind this also. The July 4th greeting card had more than 250 sites that were hosting a variety of malicious code. The Websites are using the exact same JavaScript obfuscation technique and exploit code as the greeting card run also. All e−mails use URLs that send users to an IP address that will attempt to exploit the users if their browsers are vulnerable. If the browser is not vulnerable the exploit code will not work, however the page will attempt to get the user to download a file called patch.exe by displaying a message: "If your download does not start in approximately 15 seconds click here to download." Subject lines Websense has seen so far are: a) Virus Detected!; b) Trojan Alert!; c) Worm Alert!; d) Worm Activity Detected!
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=786

28. *July 08, ComputerWorld* — **China claims Motorola, Nokia batteries explode.** As investigations continued into the death a 22−year−old Chinese man whose cell phone exploded, Chinese authorities have found batteries that may blow up when used in Motorola Inc. and Nokia Corp. cell phones, news reports said Friday, July 6. Government regulators in the southern province of Guangdong said this week that they had discovered unsafe Motorola and Nokia mobile phone batteries that could explode under certain conditions, the New York Times, Bloomberg, and the Chicago Tribune reported. Both handset manufacturers have said they are cooperating with the safety investigation, but claimed that the batteries fingered by authorities were unauthorized copycats. The news adds a turn to the ongoing investigation of the June 19 death of Xiao Jinpeng, a 22−year−old welder who died after the battery in his handset apparently exploded. However, neither Motorola or provincial law enforcement has confirmed that the phone, reported as made by Illinois−based Motorola, was actually a company−branded handset.
Source: http://www.computerworld.com/action/article.do?command=viewA rticleBasic&articleId=9026498&intsrc=hm_list

29. *July 06, Linux Devices* — **New FCC rules may impact Linux−based devices.** New U.S. regulations went into effect Friday, July 6, that could change how vendors of devices with software−defined radios (SDR) use open−source software. The new rules could impact manufacturers of mobile phones, Wi−Fi cards and other devices that use SDR technologies. SDR technologies are commonly used in today's mobile phones and Wi−Fi equipment. The Federal Communications Commission's (FCC) new regulations are apparently aimed at ensuring that users of such equipment cannot access source code needed to reprogram it −− for example, to output more power, or operate on inappropriate frequencies, either of which could conceivably endanger public safety. A summary document published by the FCC suggests that because of the new rules, SDR device vendors who use open−source software in certain capacities could face challenges getting FCC approval.
FCC 2500−word document: http://edocket.access.gpo.gov/2007/07−2684.htm
Source: http://linuxdevices.com/news/NS9075126639.html

30. *July 06, IDG News Service* — **Yahoo sites hit by availability problems.** Yahoo Inc. suffered availability problems on Friday, July 6, that affected its home page as well as other of its

Websites and services for a sustained period of time. Yahoo, which has some of the most popular sites and online services worldwide, first experienced problems on its home page at around 5:50 a.m. U.S. Pacific Time, said Dan Berkowitz, senior communications director at Keynote Systems Inc. Yahoo.com's operations began getting back to normal at around 7:15 a.m., said Berkowitz. At its worst point, Yahoo.com's availability dropped to around 60 percent, meaning that four out of ten visitors couldn't access the page, he said. A variety of bloggers also reported trouble Friday morning accessing other Yahoo services like Yahoo Messenger and Yahoo Mail, as well as other Yahoo sites like the Flickr photo sharing site and the news aggregation site Yahoo News.
Source: http://www.infoworld.com/article/07/07/06/Yahoo−sites−hit−by−availability−problems_1.html

31. *July 06, ENN (Ireland)* — **U.S. claims top spam spot.** The U.S. was top of the spam charts for the month of June, according to new e−mail security statistics from IE Internet. The U.S. generated 37.4 percent of all spam filtered by Irish security and e−mail monitoring firm IE Internet during the month of June, well clear of the chasing pack. China came in second with responsibility for 17 percent of spam sent to Irish firms, followed by the UK in third place on 10.9 percent. Mexico claimed fourth place with 9.9 percent, while Russia rounded out the top five, accounting for 7.6 percent of all spam.
Source: http://www.enn.ie/article/65402.html

32. *July 05, Information Week* — **Downed electronic jihad site flew under the radar.** Although the "electronic jihad" Website Al−jinan.org was offline for part of Thursday, July 5, the site has been able to survive for about four−and−a−half years for a number of reasons. While its domain name server registration features a number of contradictions that make tracing its origins difficult, the capabilities of the site's Electronic Jihad application are also limited. Still, the mere presence of the site is likely a precursor of an emerging cyber threat. Al−jinan.org's domain name server is being hosted by Ibtekarat, a Web hosting company based in Beirut. Created in December 2002, the site's registration information cites an address with a Los Angeles postal code, while listing the Egyptian city of Al Esmaeiliya as its "registrant city," and Iraq as its "registrant country." Anyone can register as a user with the Al−jinan.org Website and install the Electronic Jihad application on their computer. This gives the user the ability to launch denial−of−service attacks using their own computing resources, although the severity of such an attack depends upon the attacker's resources. According to claims posted on Al−jinan.org, they have contributed to knocking offline various Websites they deem as anti−Islamic.
Source: http://www.informationweek.com/software/showArticle.jhtml;jsessionid=MJ0IVBHGJFEHUQSNDLRCKH0CJUNN2JVN?articleID=200900590&articleID=200900590

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

33. *July 09, New York Times* — **New York plans surveillance veil for downtown.** By the end of this year, police officials say, more than 100 cameras will have begun monitoring cars moving through Lower Manhattan, the beginning phase of a London−style surveillance system that would be the first in the United States. The Lower Manhattan Security Initiative, as the plan is called, will resemble London's so−called Ring of Steel, an extensive web of cameras and roadblocks designed to detect, track, and deter terrorists. British officials said images captured by the cameras helped track suspects after the London subway bombings in 2005 and the car bomb plots last month. If the program is fully financed, it will include not only license plate readers but also 3,000 public and private security cameras below Canal Street, as well as a center staffed by the police and private security officers, and movable roadblocks. Three thousand surveillance cameras would be installed below Canal Street by the end of 2008, about two−thirds of them owned by downtown companies. Pivoting gates would be installed at critical intersections; they would swing out to block traffic or a suspect car at the push of a button Critics question the plan's efficacy and cost.
Source: http://www.nytimes.com/2007/07/09/nyregion/09ring.html?_r=1& hp&oref=slogin

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer